Account Manipulation: Additional Container Cluster Roles, Sub-technique T1098.006 - Enterprise

Archived: 2026-04-05 18:16:52 UTC

An adversary may add additional roles or permissions to an adversary-controlled user or service account to maintain persistent access to a container orchestration system. For example, an adversary with sufficient permissions may create a RoleBinding or a ClusterRoleBinding to bind a Role or ClusterRole to a Kubernetes account.[1][2] Where attribute-based access control (ABAC) is in use, an adversary with sufficient permissions may modify a Kubernetes ABAC policy to give the target account additional permissions.[3]

This account modification may immediately follow Create Account or other malicious account activity. Adversaries may also modify existing Valid Accounts that they have compromised.

Note that where container orchestration systems are deployed in cloud environments, as with Google Kubernetes Engine, Amazon Elastic Kubernetes Service, and Azure Kubernetes Service, cloud-based role-based access control (RBAC) assignments or ABAC policies can often be used in place of or in addition to local permission assignments.[4][5][6] In these cases, this technique may be used in conjunction with Additional Cloud Roles.

Source: https://attack.mitre.org/techniques/T1098/006